

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

09/27/2019

SUBJECT:

A Vulnerability in vBulletin Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in vBulletin which could allow for remote code execution when a malicious POST request is sent to the vulnerable application. vBulletin is a software package written in PHP used to create forums. Successful exploitation of this vulnerability could enable the attacker to perform system command execution in the context of the web server hosting the application. Depending on the privileges associated with the vBulletin service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights

THREAT INTELLIGENCE:

There are reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- vBulletin versions 5.0.0 to 5.5.4

RISK:

Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: NA

TECHNICAL SUMMARY:

A vulnerability has been discovered in vBulletin which can allow for remote code execution when a malicious POST request is sent to the vulnerable application. This vulnerability exists due to improper input validation within the widgetConfig[code] parameter when a POST request is sent to the index page of the vBulletin with the routestring, "ajax/render/widget_php". An attacker can load an arbitrary widget and run code provided within the widgetConfig[code] parameter. Depending on the privileges associated with the vBulletin service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by vBulletin to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

vBulletin:

https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4422707-vbulletin-security-patch-released-versions-5-5-2-5-5-3-and-5-5-4

SecList:

<https://seclists.org/fulldisclosure/2019/Sep/31>

Ars Technica:

<https://arstechnica.com/information-technology/2019/09/public-exploit-code-spawns-mass-attacks-against-high-severity-vbulletin-bug/>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16759>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts

Security Operations Analyst

MS Department of Information Technology Services

601-432-8201 | www.its.ms.gov





DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited